A Data Hiding Technique

KEYWORDS

Prof. Ravi S. Shrivas	Gayatri Manikrao Gore
Eletronics and Telecommunication Jahawarlal Darda Institute Of Engineering And Technology Yavatmal India	Eletronics and Telecommunication Jahawarlal Darda Institute Of Engineering And Technology Yavatmal India

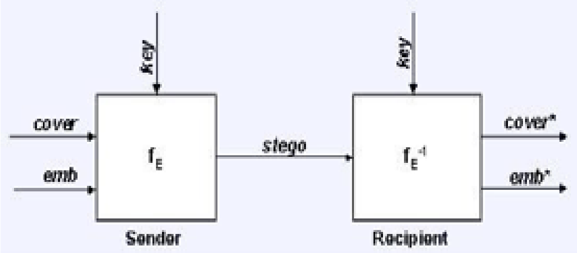
ABSTRACT *Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. Steganography is a useful tool that allows covert transmission of information over the communication channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval. This method can be used for announcing a secret message in public place. It increased the level of information security with a wide use of its techniques. It would be very useful and provide a better platform for the beginners who want to work in steganography. By analyzing the existing techniques more new techniques can be developed.*

Introduction

Steganography is the art and science of hiding information by embedding data into cover media. The term originated from Greek roots that literally mean "covered writing" .This idea was first described by Simmons in 1983. Steganography is different from cryptography which is about concealing the content of message whereas steganography is about concealing the existence of the message itself .

Traditional methods were being used, before the invention of digital means for sending or receiving messages. Before phones, mail messages were sent on foot. With the rapid growth of the Internet and multimedia systems in distributed environments, it becomes very difficult to transfer the data securely. Steganography and Cryptography provides helps us to cross this type of hurdle. Steganography plays an important role in information security and hence widely used than cryptography now days. Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav.. These formats are also popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message. Steganographic technologies are a very important part for Internet security in the future of and privacy on open systems such as the Internet. Due to the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open-systems environment, steganographic research is primarily driven .

In steganography, the possible cover carriers are the carriers (images, audio, video, text, or some other digitally representative code) that holds the hidden information. A message is the information hidden which may be cipher text, images, plaintext, or anything that can be embedded into a bit stream. The cover carrier and the embedded message together create a stego-carrier. Hiding information require a stego key which is the additional secret information, such as a password is required for embedding the information. For example, when a secret message within a cover image is hidden, the resulting product is said to be stego-image. A possible formula of the process is given as:



fE : steganographic function "embedding"
fE-1 : steganographic function "extracting"
cover: cover data in which the message *emb* will be hidden
emb: message that is to be hidden
stego: cover data with the hidden message

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Using encryption might identify the sender or receiver as somebody with something to hide. For example, the picture of our cat could conceal the plans for our company's latest technical innovation. Encryption allows communication to be secure requiring a key to read the information. An attacker cannot remove the encryption but it can easily make modifications in the file by making it unreadable for the intended recipient.

LITERATURE REVIEW

The word Steganography comes from the Greek origin that means "covered(concealed) writing". The word "steganos" means "protected or covered" and "graphie" means "writing". Steganography thus not only emphasizes on the art of hiding information but also the art and science of hiding the communication that takes place. A Greek historian Herodotus gave the first application of Steganography. In his history of the Persian Wars, Herodotus gives an example of a messenger who shaved his head and allowed a secret message that was to be send to be tattooed on his scalp. He waited for his hair to grew back and then journeyed where the recipient awaited him and shaved his head again. The message was revealed. It was considered as history's first use of steganography. This method has various drawbacks, such as delayed transmission while waiting for hair to grow and limited size also .The next steganography method that was used during those days is tablet wax. The tablet was erased by wax in order to hide the message and text was etched on and then again covered it by wax and appeared blank upon inspections. During the century, the methods of using invisible inks were extremely popular. During the World War II, it was true that people used ink for writing hidden messages. On heating, the mixture turn darker and the written messages becomes visible. After some time, the Germans introduced the microdot technique where microdots are considered as photographs being as small as a printed period and with a clear format of a typewritten page. They were included in an envelope or a letter, and because of their tiny sizes, they could be unable to see. Microdots were also hidden in body parts including nostrils, ears, or under fingernails .The military and several governmental agencies are looking into steganography for their own secret transmissions of information. They are also desiring of discerning secret information communicated by terrorists, criminals, and other aggressive forces .

WHAT IS CRYPTOGRAPHY?

Cryptography is said to be as the science of information security. The word is derived from the Greek word *kryptos*, which means hidden. Cryptography is closely related to the disciplines of cryptanalysis and cryptology . Cryptography includes techniques such as merging words with images, microdots and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling i.e. mixing of plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), and then back again (known as decryption).

Comparision of Steganography and Cryptography:

Steganography and cryptography are closely related. Cryptography scrambles messages so that others may not be able to understand about it. On the other hand, steganography hide the message so there is no knowledge of the existence of the message. Comparison is made between portions of the cipher text and that of portions of the plaintext with cryptography. In steganography, comparisons may be made between the stego-media and cover-media, and possible portions of the message. The cipher text is the end result in cryptography, while in steganography, the end result is the stego-media. The message in steganography may be encrypted or may not be encrypted. If it is encrypted, then a technique known as cryptanalysis is applied to extract the message.

Those who seek the ultimate in private communication can combine steganography and encryption. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text in the carrier medium. There are several tools by which encryption of data can be done before hiding it in the chosen medium. Both methods can be combined to produce better protection of the message. In case, if the steganography fails and the message can be detected, it is still of no use as it is being encrypted using the cryptography techniques [4].

HOW IT WORKS?

Modern Steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements :

· The cover media(*C*) that will hold the hidden data

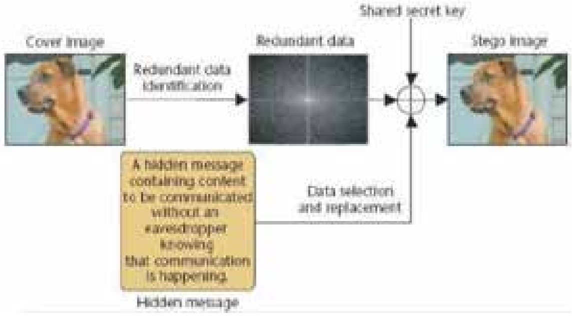
· The secret message (*M*), may be plain text, cipher text or any type of data

· The stego function (*Fe*) and its inverse (*Fe-1*)

· An optional stego-key (*K*) or password may be used to hide and unhide the message.

The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media (*S*). The functioning of steganographic operation is shown below.

FIGURE II : The steganographic operation


Shared secret key
Cover image
Redundant data
Stego image
Redundant data identification
A hidden message containing content to be communicated without an eavesdropper knowing that communication is happening
Data selection and replacement
Hidden message

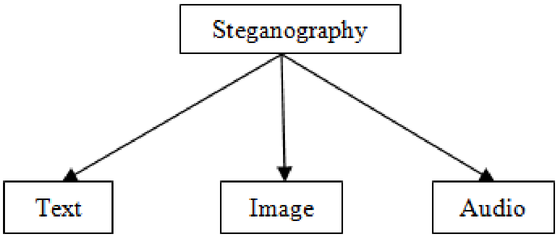
Steganography and Cryptography are great partners in spite of functional difference. It is common practice to use cryptography with Steganography [6].

STEGANOGRAPHY METHODS

There exist two types of materials in steganography: message and carrier. The secret data that is to be hidden is said to be message and the material that takes the message in it is a carrier .

There are many types of steganography methods. Let's take a short look at different steganography methods. Figure below shows the different types of steganography techniques .

FIGURE III : Steganography types diagram



Text Steganography

Text steganography can be achieved by altering certain characteristics of textual elements (e.g., characters) or altering the text formatting, or The goal in the design of coding methods is to develop alterations that are reliably decidable (even in the presence of noise) yet largely indiscernible to the reader. These criteria, reliable decoding and minimum visible change, are somewhat conflicting; herein lies the challenge in designing document marking techniques. The three coding techniques that we propose illustrate different approaches rather than form <an exhaustive list of document marking techniques. The techniques can be used either separately or jointly. Each technique enjoys certain advantages or applicability as we discuss below [6].

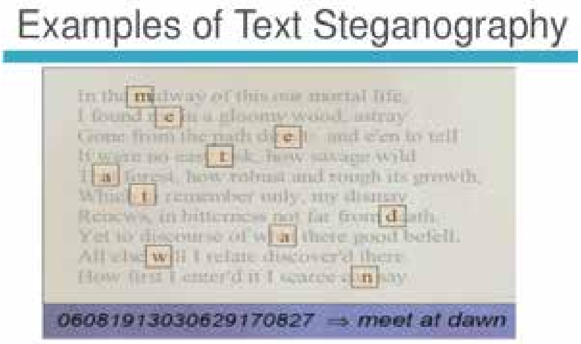
Line-shift coding

This is a method of altering a document by vertically shifting the locations of text lines to encode the document uniquely. This encoding may be applied either to the format file or to the bitmap of a page image. The embedded codeword may be extracted from the format file or bitmap. In certain cases this decoding can be accomplished without need of the original image, since the original is known to have uniform line spacing between adjacent lines within a paragraph [6].

Word-shift coding

This is a method of altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely. This encoding can be applied to either the format file or to the bitmap of a page image. Decoding may be performed from the format file or bitmap. The method is applicable only to documents with variable spacing between adjacent words. Variable spacing in text documents is commonly used to distribute white space when justifying text. Because of this variable spacing, decoding requires the original image - or more specifically, the spacing between words in the un-encoded document [6].

FIGURE IV : Image using word shift coding



Examples of Text Steganography

In the midway of this our mortal life
I found me in a gloomy wood, astray
Gone from the path direct: and e'en to tell
It were no easy task, how savage wild
That forest, how robust and rough its growth,
Which to remember only, my dismay
Renews, in bitterness not far from death.
Yet to discourse of what there good befell,
All else will I relate discover'd there.
How first I enter'd it I scarce can say

06081913030629170827 → meet at dawn

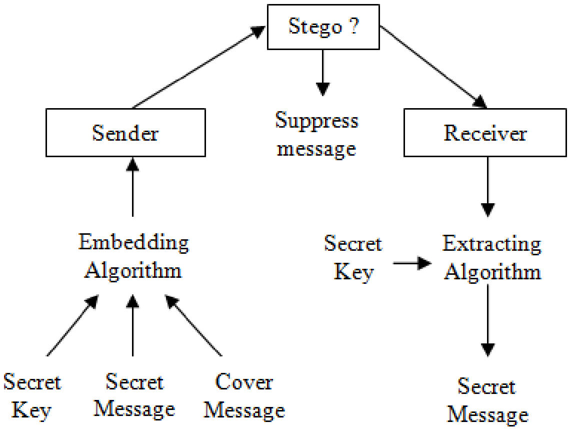
Feature coding

This is a coding method that is applied either to a format file or to a bitmap image of a document. The image is examined for chosen text features, and those features are altered, or not altered, depending on the codeword. Decoding requires the original image, or more specifically, a specification of the change in pixels at a feature. There are many possible choices of text features; here, we choose to alter upward, vertical endlines - that is the tops of letters, b, d, h, etc. These endlines are altered by extending or shortening their lengths by one (or more) pixels, but otherwise not changing the endline feature . There is another form of text steganography which is defined by Chapman et al. as the text steganography is a method of using written natural language to conceal a secret message[6].

Image Steganography

Nowadays the most popular technique used for hiding information is image steganography. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert Niels Provos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited. To hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy" areas with many colour variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files[5].

FIGURE V : General Steganographic Approach.



Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the "noise" level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used [5].

Various techniques of image steganography

LSB method

The popular and oldest method for hiding the message in a digital image is the LSB method. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small . To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(0010011**1** 1110100**0** 1100100**0**)

(0010011**0** 1100100**0** 1110100**0**)

(1100100**0** 0010011**1** 11101001)

In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden . As you see, the least significant bit of third color is remained without any changes. It can be used for checking the correctness of 8 bits which are embedded in these 3 pixels. In other words, it could be used as "parity bit"[7].

Another example we can take is that data bits 01100101 are tried to hide into an 8 bit colour image. According to this technique 8 consecutive pixels from top left corner of the image are selected. The binary equivalent of those pixels may be like this:

00100101 11101011 11001010 00100011

11111000 11101111 11001110 11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern would become:

0010010**0** 1110101**1** 1100101**1** 0010001**0**

1111100**0** 1110111**1** 1100111**0** 1110011**1**

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise[5].

Advantages of LSB
100 % chances of insertion.
Easy to implement.
Disadvantages of LSB

One of the major disadvantage associated with LSB method is that intruder can change the least significant bit of all the image pixels. In this way hidden message will be destroyed by changing the image quality, a little bit, i.e. in the range of +1 or -1 at each pixel position. Not immune to noise and compression technique[7].

Local pixel adjustment technique

Local Pixel adjustment process improves the image quality of the stego-image. Local pixel adjustment process only considers the last three significant bits and the fourth bit but not all bits. The local pixel adjustment method is not optimal. As the local Pixel Adjustment process modifies the LSBs, the technique cannot be applied to data hiding schemes based on simple LSB substitution[1].

Optimal pixel adjustment technique

This is the technique given by Chan et. al in 2003. This is a data hiding scheme which uses simple LSB substitution with an optimal pixel adjustment process. This method provides less change in image quality as compared to the LSB Method and local pixel adjustment process (LPAP). The image quality of the stego-image is improved by using this method[1].

6th,7th and 8th bit method

In this method 6th, 7th and 8th bits of the image pixels are used to hide the message. Since this method involves 8th bit for hiding the message, intruder can easily change 8th bit of all image pixels and this may result in the loss of message. To avoid this, time factor has been introduced, i.e. at some time t1, sender sends the cover object with message and at some other time t2 sender sends the cover object without message. Sender and recipient agree on this time factor initially before starting any communication. The advantage of introducing time factor (slot) is that if least significant bits of all pixels are changed by the intruder even then the message can be retrieved by comparing the two cover objects, i.e. one containing the message and the other not containing the message[1].

Parity checker method

According to this method, 0 can be inserted at a pixel location if that pixel has odd parity i.e. the number of 1's in the binary value of the pixel should be odd. Similarly, 1 can be inserted at a pixel location if that pixel has even parity i.e. the number of 1's in the binary value of pixel should be even. If the corresponding parity does not exist at a pixel location either for 0 or 1, then we make corresponding parity at that pixel location (odd parity for 0 and even parity for 1) by adding or subtracting 1 to the pixel location such that the change in the image quality should not be visible to the human visual system (HVS)[1].

PVD method

The pixel value differencing (PVD) method proposed by Wu and Tsai can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification[1].

Tri-way PVD method

This method is an improvement of the PVD method in terms of hiding capacity. In PVD method, only one direction is referenced whereas in this method three directional edges i.e. horizontal, vertical and diagonal edges are taken into consideration in order to hide the secret data bits. At first, the entire cover image is divided into a number of non-overlapping 2X2 blocks. Three pixel pairs of each block aroused for embedding purpose. The pixel pair that is taken into consideration is in the horizontal, vertical and diagonal directions. Data bits are embedded on the basis of the difference between the two pixel values of each pixel pair[1].

Audio Steganography

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. We are going to have a brief introduction on some of them.

LSB coding

Sampling technique followed by Quantization converts analog audio signal to digital binary sequence. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.

Phase coding

Human Auditory System (HAS) can't recognize the phase change in audio signal as easy it can recognize noise in the signal. The phase coding method exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to- noise ratio.

Spread Spectrum

There are two approaches are used in this technique: the direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). Direct-sequence spread spectrum (DSSS) is a modulation technique used in telecommunication. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated. Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudorandom sequence of 1 and −1 values, at a frequency much higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band. The resulting signal resembles white noise. However, this noise-like signal can be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence (because 1 × 1 = 1, and −1 × −1= 1). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted Pseudorandom Noise (PN) sequence with the receiver's assumed sequence. For de-spreading to work correctly, transmit and receive sequences must be synchronized. This requires the receiver to synchronize its sequence with the transmitter's sequence via some sort of timing search process. In contrast, frequency-hopping spread spectrum pseudo-randomly retunes the carrier, instead of adding pseudo-random noise to the data, which results in a uniform frequency distribution whose width is determined by the output range of the pseudo-random number generator .

Echo hiding

In this method the secret message is embedded into cover audio signal as an echo. Three parameters of the echo of the cover signal namely amplitude, decay rate and offset from original signal are varied to represent encoded secret binary message. They are set below to the threshold of Human Auditory System (HAS) so that echo can't be easily resolved. Video files are generally consists of images and sounds, so most of the relevant techniques for hiding data into images and audio are also applicable to video media. In the case of Video steganography sender sends the secret message to the recipient using a video sequence as cover media. Optional secret key 'K' can also be used during embedding the secret message to the cover media to produce 'stego-video'. After that the stego-video is communicated over public channel to the receiver. At the receiving end, receiver uses the secret key along with the extracting algorithm to extract the secret message from the stego-object[5].

STAGANALYSIS

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes". It is the art of discovering and rendering useless covert messages. The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information. Unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message. Steganalysis generally starts with several suspect information streams but uncertainty whether any of these contain hidden message. The steganalyst starts by reducing the set of suspect information streams to a subset of most likely altered information streams. This is usuallydone with statistical analysis using advanced statistics techniques.

Steganalysis Techniques

Hiding information within an electronic medium cause alteration of the medium properties that can result in some form of degradation or unusual characteristics.

Unusual patterns

Unusual patterns in a stego image are suspicious. For example, there are some disk analysis utilities that can filter hidden information in unused partitions in storage devices. Filters can also be used to identify TCP/IP packets that contain hidden or invalid information in the packet headers. TCP/IP packets used to transport information across the Internet have unused or reserved space in the packet headers.

Visual detection

Analyzing repetitive patterns may reveal the identification of a steganography tool or hidden information. To inspect these patterns an approach is to compare the original cover image with the stego image and note visible differences. This is called a known-carrier attack. By comparing numerous images it is possible that patterns emerge as signatures to a steganography tool. Another visual clue to the presence of hidden information is padding or cropping of an image. With some stego tools if an image does not fit into a fixed size is cropped or padded with black spaces. There may also be a difference in the file size between the stego-image and the cover image. Another indicator is a large increase or decrease in the number of unique colors, or colors in a palette which increase incrementally rather than randomly.

Tools to detect steganography

The disabling or removal of hidden information in images is dependent on the image processing techniques. For example, with LSB methods of inserting data, simply compressing the image using lossy compression is enough to disable or remove the hidden message.

APPLICATIONS OF STEGANOGRAPHY

Steganography is used in a lot of useful applications:

- Smart identity cards where the details of individuals are embedded in their photographs.
- Video-audio synchronization
- TV broadcasting
- TCP/IP packets where a unique ID is embedded in an image to analyse the network traffic of particular users .
- Medical Imaging Systems is one of the modern applications that use Steganography where a separation is recommended between patients" image data or DNA sequences and their captions for security or confidentiality reasons. Thus, embedding the patient's information in the image could be a security measure to help solving security issues .
- Steganography can be a solution that makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us[3].
- It is also possible to store information on a location simply by steganography. For example, most of the information sources like our private banking information, some military secrets, can also be stored in a cover source. When the requirement is to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside.
- Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, steganographic methods can be used to hide this.
- E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint via steganography, allow for a very secure option to open ecommerce Transform verification.
- Paired with existing communication methods, steganography can be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital steganography provides vast potential for both types. Businesses may have similar concerns regarding trade secrets or new product information.
- The transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites[3].

ADVANTAGES AND DISADVANTAGES

Advantages

1) The main advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered.

2) It keeps the message as top secret,such that apart from the sender and receiver nobody can retrieve the message.

3) Without knowing the extracting process the receiver will not be able to open the message that is hidden , it means that no unknown person can extract the data like a thief .

4) It hides the image such as text, audio, video.

5) Used by Intelligence Bureau – To send their Secret messages.

Disadvantages

1) Steganography is used by the terrorists. In 9/11 attack al-Qaeda head Bin Laden used this technology.

2) In an image he encoded whole message and then transport it via e-mail.

THE FUTURE OF STEGANOGRAPHY

Our ability to discover hidden information during our investigations is essential, especially as new and innovative methods continue to evolve.

During the past decade, data hiding technologies have advanced from limited use to ubiquitous deployment. With the rapid advancement of smart mobile devices, the need to protect valuable information has generated excess of new methods and technologies for both good and evil. Most dangerous among these are those that employ hiding methods along with cryptography, thus providing a way to both conceal the existence of hidden information while strongly protecting the information even if the channel is discovered.

It is well accepted though, small sentences and one-word answers example a "yes" are virtually impossible to find. This could be an area for further advances as possible compression sizes decreases further. There also seems very little in terms of tools for hiding data in videos. There are some for audio, but this is still an area, which lags behind image steganography. The future may see audio files and video streams that could possibly be decoded on the fly to form their correct messages.

Many vendors provide excellent technologies for protecting the privacy of information for the desktop. In addition, many of the latest smart mobile platforms (Android and iPhone) include built-in cryptographic capabilities. What is more dangerous and difficult to discover/decipher are data hiding methods that exploit multimedia and protocol weaknesses to both hide and communicate covertly. These new techniques provide hybrid solutions that combine the best of cryptography with the best of steganography. The interest, innovation, and advancement of these threats continue to go unchecked for the most part.

CONCLUSION

The various steganography methods are being analysed. Firstly, we analyze the three existing methods. After analyzing, it is found that a lot of work has been done in the field of Steganography as well as in Image Steganography. It is observed that most of the Steganography techniques are suitable to hide data either text or binary message. Image steganography is most popularly used technique in comparison with text and audio steganography. At the starting period of 2003 researchers showed least interest in steganography but as time passes the level of their interest raises, in 2012 and 2013 researchers shown much interest. It was also seen that most widely used technique was the LSB technique, Each method in image stegnography has some improvement with respect to that of the earlier method. There is always some space of improvement in mostly proposed techniques. So, in future we will try to propose some new techniques which will improve various image steganography parameters.

REFERENCE

1) Rajkumar Yadhav, Int, " Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters" . J. Comp. Tech. Appl., Vol 2 (6),1867-1870. | 2) SANS Institute InfoSec Reading Room, "A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment". | 3)Arvind kumar and pooja, "Steganography- A Data Hiding Technique" International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010 . | 4)Shilpa Thakar & Monika aggrawal " A Review –Steganography." Volume 3, Issue 12, December 2013 , International Journal of Advanced Research,Available online at www.ijarcsse.com | 5) Ronak Karimi, Mehdi Hariri & Masoud Nosrati , " An introduction to steganography methods". | World Applied Programming, Vol (1), No (3), August 2011. www.waprogramming.com | 6) Vipul Singhal, Dhananjay Yadav & Devesh Kumar Bandil,, "Steganography and Steganalysis: A Review" International Journal of Electronics and Computer Science Engineering, Available Online at www.ijecse.org. | 7) World Applied Programming, Vol (1), No (4), October 2011. ©2011 WAP journal. www.waprogramming.com ., "Embedding Stego-Text in Cover Images Using linked List Concepts and LSB Technique". | 8) Vipul Sharma & Sunny Kumar,"A New Approach to Hide Text in Images Using Steganography" Volume 3, Issue 4, April 2013 , International Journal of Advanced Research. Research Paper Available online at: www.ijarcsse.com | 9) B.Ramesh Kumar, K.Suresh, S.K.Basheer and M. Raja Krishna Kumar, "Enhanced Approach to Steganography Using Bitplanes". | 10) Samir Kumar Bandyopadhyay Senior Member IEEE An Alternative Approach of Steganography using Reference Image." International Journal of Advancements in Technology http://ijict.org/, |